Annual Report for Period: 02/2010 - 01/2011
Submitted on: 12/02/2010
Principal Investigator: Boldyreva, Alexandra .
Award ID: 0545659
Organization: GA Tech Res Corp - GIT
Submitted By:
Boldyreva, Alexandra - Principal Investigator
Title:
CAREER: Integrating Cryptography with Emerging Security Applications

Project Participants

Senior Personnel

Name: Boldyreva, Alexandra
Worked for more than 160 Hours: Yes
Contribution to Project:

Post-doc

Name: Yum, Dae Hyun
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Fehr, Serge
Worked for more than 160 Hours: Yes
Contribution to Project:
No support

Graduate Student

Name: O'Neill, Adam
Worked for more than 160 Hours: Yes
Contribution to Project:
Adam has been supported by the project funding for one semester. He is my main collaborator in research on efficiently searchable encryption.

Name: Kumar, Virendra
Worked for more than 160 Hours: Yes
Contribution to Project:

Name: Gentry, Craig
Worked for more than 160 Hours: No
Contribution to Project:

Name: Goyal, Vipul
Worked for more than 160 Hours: Yes
Contribution to Project:
No support, a collaborator

Name: Cash, David
Worked for more than 160 Hours: Yes
Contribution to Project:

Undergraduate Student

Technician, Programmer

Other Participant

Name: Bellare, Mihir

Worked for more than 160 Hours: Yes

Contribution to Project:

Mihir is a collaborator in research on efficiently searchable encryption. He is not supported by my grant.

Name: Warinschi, Bogdan

Worked for more than 160 Hours: Yes

Contribution to Project:

Bogdan is a collaborator in research on PKI security. He is not supported by my grant.

Name: Fischlin, Marc

Worked for more than 160 Hours: Yes

Contribution to Project:

Marc is a collaborator in research on PKI security and studying the gap between the standard and the random-oracle security models. He is not supported by my grant.

Name: Palacio, Adriana

Worked for more than 160 Hours: Yes

Contribution to Project:

Adriana is a collaborator in research on PKI security. She is not supported by my grant.

Name: Shi, Weidong

Worked for more than 160 Hours: Yes

Contribution to Project:

Weidong is my main collaborator in research on securiring applications in computer architecture and graphics. He is not supported by my grant.

Name: Lee, Hsien-Hsin

Worked for more than 160 Hours: Yes

Contribution to Project:

Hsien-Hsien is a collaborator in research on securiring applications in computer architecture and graphics. He is not supported by my grant.

Research Experience for Undergraduates

Organizational Partners

University of California at San Diego

University of Bristol, UK

Darmstadt University

Bowdoin College

POSTECH

Other Collaborators or Contacts

Vipul Goyal, a graduate student from UCLA,
Serge Fehr from CWI

Activities and Findings

Research and Education Activities:

Following the proposal, my recent research focused on several emerging
applications in need of cryptographic solutions, such as securing
outsourced database management, supporting authenticity in network routing protocols, adding accountability to networking applications, on-chip software execution and
digital right protection of computer graphics.

I also studied various security issues of several standardized protocols, such as OAEP and Kerberos.

Research I undertook included close collaborations with specialists in these disciplines. I and the involved graduate students interacted with professors and students at the College of Computing and the ECE department at Georgia Tech to learn better about the emerging security applications in their areas and to validate the ideas.

The research, fully or partially funded by this award has resulted in 14 publications, many of which are in top-tier conference proceedings.

We gave invited talks at Microsoft Research (California and Redmond), IBM Research, Symantech, Johns Hopkins University, Ibaraki University and AIST, Japan on our findings about deterministic encryption and securing outsourced databases. I give invited lectures on the topic at the Computer Security and cryptography workshop in Montreal, Canada in April 2010 and at the Selected areas in Cryptography (SAC' 10) conference in Waterloo, Canada in August 2010.

My education activities include my regular teaching of the graduate-level course on Applied Cryptography. I completely re-designed this course to reflect on the modern provable security methodology. I also participated in meetings with and gave lectures to middle and high school students interested in cryptography.

Findings:

We developed a new framework that allows us to design and analyze practical, provably-secure schemes that permits sublinear-time processing of exact-match queries by an untrusted server in the public-key and symmetric-key setting. The schemes provide various tradeoffs among security, functionality, and client-and-server-computation- and bandwidth-efficiency. Our security definitions are novel and can also be useful for analyzing other systems-security and cryptographic applications. There is interesting theory underlying this practical research. Namely, we provide the first definition of security for deterministic public-key encryption and provide provably-secure schemes. First we find schemes that are only secure in the idealized random oracle (RO) model. Further, we find schemes that are secure in the standard (RO devoid) model, for a slightly stronger requirement on the message space.

Next we look at a different query functionality, namely range queries. To help implement such queries efficiently on encrypted data in the most practical symmetric-key setting we study the notion of deterministic order-preserving encryption (OPE). We investigate what level of security can order-preserving schemes provide, and formulate several security definitions. Then we present the first provably secure order-preserving encryption scheme.

However our new security notion is not completely satisfactory in that it is unclear what information ``ideal object'' leaks about the underlying data. In the follow-up work we provide results that better characterize the information leakage of the best possible order-preserving encryption.We also propose several ways to improve security of encryption suitable for answering range queries.
We show that a stronger security level be achieved in certain situations, namely if the data is known completely in advance or if the server uses a secure hardware.
We propose a modification to our previous OPE scheme and show that it avoids leakage of plaintext location.

We also presented a novel protection model for proprietary graphics data by
integrating cryptographic solutions for digital rights management into the graphics processing

unit and creating a digital rights enabled graphics processing system to defend piracy of entertainment software and copyrighted graphics arts.

We constructed new multiparty signature schemes that allow multiple signers to sequentially produce a compact, fixed-length signature. We focused on applications of our schemes to secure network routing, but we believe they would find many other applications as well. First, we introduce a new public-key primitive that we call ordered multisignatures (OMS), which allows signers to attest to a common message as well as the order in which they signed. Our OMS construction substantially improves computational efficiency over any existing scheme with suitable functionality. Secondly, we design a new identity-based sequential aggregate signature scheme, where signers can attest to different messages and signature verification does not require knowledge of traditional public keys. The latter property permits savings on bandwidth and storage as compared to public-key solutions. In contrast to the only prior scheme to provide this functionality, ours offers improved security that does not rely on synchronized clocks or a trusted first signer. We provide formal security definitions and support the proposed schemes with security proofs under appropriate computational assumptions.

Kerberos is a widely-deployed network authentication protocol that is being considered for standardization. Many works have analyzed its security, identifying flaws and often suggesting fixes, thus helping the protocol's evolution. Several recent results present successful formal-methods-based verification of a significant portion of the current version 5, and some even imply security in the computational setting. For these results to be meaningful, encryption in Kerberos should satisfy strong cryptographic security notions. However, neither currently deployed as part of Kerberos encryption schemes nor their proposed revisions are known to provably satisfy such notions. We take a close look at Kerberos' encryption and confirm that most of the options in the current version provably provide privacy and authenticity, some with slight modification that we suggest. Our results complement the formal-methods-based analysis of Kerberos that justifies its current design.

Currently, the best and only evidence of the security of the OAEP encryption scheme is a proof in the contentious random oracle model. We give further arguments in support of the security of OAEP. We first show that partial instantiations, where one of the two random oracles used in OAEP is instantiated by a function family, can be provably secure (still in the random oracle model). For various security statements about OAEP we specify sufficient conditions for the instantiating function families that, in some cases, are realizable through standard cryptographic primitives and, in other cases, may currently not be known to be achievable but appear moderate and plausible. Furthermore, we give the first non-trivial security result about fully instantiated OAEP, where both oracles are instantiated simultaneously. We also discuss the implications, especially of the full instantiation result, to the usage of OAEP for secure hybrird encryption (as required in SSL/TLS, for example).
Recently, we studied security of OAEP in the practical setting where an adversary can see multiple challenge ciphertexts (previous definitions considered only one). My (and co-authors) old results imply that security of a general encryption scheme does degrade as adversaries observe more ciphertexts. We now show that an extremely simple modification to the OAEP scheme yields a scheme whose security stays the same no matter how many challenge ciphertexts adversaries observe. This modification has other advantages and is simple enough, so we believe it deserves attention of the standards bodies.

We study an issue which is critical to many applications, namely key revocation in identity-based encryption (IBE). Revocation is a well-studied problem in the traditional PKI setting. However in the setting of IBE, there has been little work on studying the revocation mechanisms. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority. We note that this solution does not scale well -- as the number of users increases, the work on key updates becomes a bottleneck. We propose an IBE scheme that significantly improves key-update efficiency on the side of the trusted party (from linear to logarithmic in the number of users), while staying efficient for the users.

OAEP is one of the few standardized and widely deployed public-key

encryption schemes. OAEP was shown to be IND-CCA secure assuming the underlying trapdoor permutation is partial one-way, and RSA-OAEP was proven to be IND-CCA under the standard RSA assumption, both in the random oracle model. However, the latter reduction is not tight, meaning that the guaranteed level of security is not very high for a practical parameter choice. We observe that the situation is even worse because both analyses were done in the single-query setting, i.e.~where an adversary gets a single challenge ciphertext. We propose a very simple modification of the OAEP encryption, which asks that the trapdoor permutation instance is only applied to a part of the OAEP transform. We show that IND-CCA security of this scheme is tightly related to the hardness of one-wayness of the trapdoor permutation in the random oracle model. We also show that security does not degrade as the number of ciphertexts an adversary can see increases.

Training and Development:

The interdisciplinary collaborations were very fruitful for all sides. We learned about the emerging applications in other areas, and the researches in these areas learned about the advanced of modern cryptography, in particular, provable security. The existing and future publications of our works should broaden this impact.

Outreach Activities:

I gave an invited talk at the RSA conference in Japan on provable security methodology and my research on security of OAEP encryption scheme. Many industry practitioners attended the talk.

I gave an invited talk at Microsoft to software engineers about the ideas and current state of provable security research in cryptography.

I participated in a meeting with minority high school students who attended a math/crypto camp and are applying to colleges.

I gave an invited talk about cryptography at the summer school for gifted middle school students in Atlanta.

Journal Publications

A. Boldyreva, M. Fischlin, A. Palacio and B. Warinschi, "A closer look at PKI: Security and Efficiency", To appear at Public Key Cryptography 2007 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, 2007., p. , vol. , (2007). Accepted,

W. Shi, H.-H. S. Lee, R. M. Yoo, and A. Boldyreva., "A Digital Rights Enabled Graphics Processing System", ACM SIGGRAPH/Eurographics Workshop of Graphics Hardware Proceedings, 2006., p. 100?, vol. , (2006). Published,

A. Boldyreva and M. Fischlin, "On the security of OAEP", Advances in Cryptology - Asiacrypt 2006 Proceedings, Lecture Notes in Computer Science,, p. 210, vol. 4284, (2006). Published,

A. Boldyreva and V. Kumar., "Provable-Security Analysis of Authenticated Encryption in Kerberos.", IEEE Security and Privacy 2007 Proceedings, p. , vol. , (2007). Published,

G. Amanatidis, A. Boldyreva and A. O'Neill., "Provably-Secure Schemes for Basic Query Support in Outsourced Databases.", Working Conference on Data and Applications Security 2007 Proceedings, Springer-Verlag, p. , vol. , (2007). Published,

M. Bellare, A. Boldyreva and A. O'Neill., "Deterministic Encryption and Sublinear-Time Keyword Search.", Advances in Cryptology - Crypto 2007 Proceedings, Lecture Notes in Computer Science, p. , vol. , (2007). Published,

M. Bellare, A. Boldyreva, K. Kurosawa and J. Staddon., " Multi-Recipient Encryption Schemes: How to Save on Bandwidth and Computation without Sacrificing Security", IEEE Transactions on Information Theory, p. , vol. , (2007). Accepted,

A. Boldyreva, C. Gentry, A. O'Neill and D. H. Yum., "Ordered Multisignatures and Identity-Based Sequential Aggregate Signatures, with Applications to Secure Routing.", ACM Conference on Computer and Communications Security (CCS '07) Proceedings, p. , vol. , (2007). Published,

Alexandra Boldyreva, Serge Fehr, Adam O'Neill, "On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles", CRYPTO 2008, p. , vol. , (2008). Published,

A. Boldyreva, V. Goyal and V. Kumar, "Identity-based Encryption with Efficient Revocation", ACM CCS, p. , vol. , (2008). Published,

Alexandra Boldyreva, Craig Gentry, Adam O'Neill, Dae Hyun Yum, "New Multiparty Signature Schemes for Network Routing Applications", ACM TISSEC, p. , vol. , (2008). Published,

A. Boldyreva, "Strengthening Security of RSA-OAEP", CT RSA, p. , vol. , (2008). Submitted,

Alexandra Boldyreva and David Cash and Marc Fischlin and Bogdan Warinschi, "Foundations of Non-Malleable Hash and One-Way Functions", Asiacrypt, p. , vol. , (2009). Accepted,

Alexandra Boldyreva and Hideki Imai and Kazukuni Kobara, "How to Strengthen the Security of RSA-OAEP", IEEE Transactions on Information Theory, p. , vol. , (2009). Published,

Alexandra Boldyreva and Nathan Chenette and Younho Lee and Adam O'Neill, "Order-Preserving Symmetric Encryption", Eurocrypt, p. , vol. 5479, (2009). Published,

Mihir Bellare; Alexandra Boldyreva; Lars Knudsen and Chanathip Namprempre, "On-line Ciphers and the Hash-CBC Constructions", Journal of Cryptology, p. , vol. , (2010). Accepted,

Books or Other One-time Publications

Web/Internet Site

URL(s):
http://www-static.cc.gatech.edu/~aboldyre/publications.html
Description:

Other Specific Products

Contributions

Contributions within Discipline:
We developed a new cryptographic primitive, efficiently-searchable encryption. That includes designing a security model and providing several constructions, both in the public-key and symmetric-key settings.

The developed theory underlying the above research included the first security definition for a public-key deterministic encryption scheme and provably-secure construction and the first definition of order-preserving encryption and provably-secure construction.

We have been studying the soundness of the controversial Random Oracle model, and its implications on the security on the most practical and standardized RSA-OAEP encryption scheme.

We designed the first formal security model for the Public Key Infrastructure (PKI).

We analyzed the encryption schemes used in Kerberos.

We studied and designed new multiparty signature schemes.

We proposed the first identity-based encryption scheme with efficient key revocation.

We studied a new security notion for hash functions -- non-malleability.

We showed that a slight modification to the standardized RSA-OAEP scheme yields multiple security improvements.

We studied order-preserving encryption with applications for range queries on encrypted databases. Proposed the first security definition and a scheme.

Contributions to Other Disciplines:

My work on securing the graphics, computer networks, computer architecture and database applications has advanced these disciplines by bringing the cryptographic schemes tailored for particular applications and supported by provable-security analysis.

Contributions to Human Resource Development:

My graduate course on Applied Cryptography and my undergraduate course on Computer and Network Security are ones of the few courses taught in the US that teach the students the basics of the provable-security methodology.

I developed a set of slides that complement the existing lecture notes. My slides include graphics and animation to help the students to grasp the complex notions of modern cryptography.

Several graduate students are involved in the projects. They have been learning a lot about cryptography and other disciplines, and more importantly, how to do good research.

I gave a talk about cryptography at the summer school for gifted middle school students in Atlanta.

Contributions to Resources for Research and Education:

Contributions Beyond Science and Engineering:

Conference Proceedings

Boldyreva, A;Chenette, N;Lee, Y;O'Neill, A, Order-Preserving Symmetric Encryption, "APR 26-30, 2009", ADVANCES IN CRYPTOLOGY - EUROCRYPT 2009, 5479: 224-241 2009

Boldyreva, A;Goyal, V;Kumar, V, Identity-based Encryption with Efficient Revocation, "OCT 27-31, 2008", CCS'08: PROCEEDINGS OF THE 15TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, : 417-426 2008

Boldyreva, A;Gentry, C;O'Neill, A;Yum, DH, Ordered Multisignatures and Identity-Based Sequential Aggregate Signatures, with Applications to Secure Routing, "OCT 29-NOV 02, 2007", CCS'07: PROCEEDINGS OF THE 14TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, : 276-285 2007

Boldyreva, A, Strengthening Security of RSA-OAEP, "APR 20-24, 2009", TOPICS IN CRYPTOLOGY - CT-RSA 2009, PROCEEDINGS, 5473: 399-413 2009

Special Requirements

Special reporting requirements: None

Change in Objectives or Scope: None

Animal, Human Subjects, Biohazards: None

Categories for which nothing is reported:

Any Book

Any Product

Contributions: To Any Resources for Research and Education

Contributions: To Any Beyond Science and Engineering